protiviti®
Global Business Consulting

COMPLIANCE INSIGHTS

不正対策とコンプライアンスの接点：より強固な防衛線の構築

Carol Beaumier、Bernadine Reese著

金融サービス業界においては、不正リスクとコンプライアンスリスク［特に、マネーロンダリング対策（AML）リスク］の管理を統合する取り組みが、過去25年にわたり進展してきました。2000年代初頭には、伝統的な銀行から保険会社に至る金融機関が、多くの場合は成功に至らなかったものの、不正とAMLリスク管理機能の統合（しばしば「FRAML」と呼ばれます）を試みた例が見られました。しかし、業界全体では、不正対策とコンプライアンスは依然として別々の分野として扱われ、正式な統合に対する業界全体の関心は限定的でした。

不正対策およびコンプライアンス分野の伝統的な定義

- 不正：財務損失やその他の全社的な損害をもたらす悪意ある行為の発見、予防、対応。
- コンプライアンス：管轄区域の法律、規制、および規則の遵守。

不正対策およびコンプライアンスリスクの統合的管理に向けた長い道のり

2010年代半ばまでに、不正対策とコンプライアンス機能の間でのより適切な連携の実現に向けた推進力が高まりました。その一因として、以下が挙げられます。

- 不正対策およびAMLチームが、同じ悪質な行為者を調査し、同じまたは少なくとも類似した脅威・リスクのタイポロジー（手口）を使用していることが、次第に認識されるようになってきたこと。
- 英国金融行動監視機構（UK FCA）や米国金融犯罪取締ネットワーク（FinCEN）などの規制当局が、AML、不正対策およびサイバーセキュリティの各機能間における、より緊密な連携を促していること。
- フィンテック企業から既存の大手プロバイダーに至るまで、あらゆる規模のテクノロジーベンダーが統合検知プラットフォームの提供を開始していること。

それでもなお、融合はほとんどが構想段階にとどまり、運用効率の向上を目的として取り組んだごく少数の大手金融機関を除けば、その融合が実現することはほとんどありませんでした。

過去3～4年間で、不正対策とコンプライアンスリスク管理の融合は、「あると望ましい」効率化施策の位置づけを超え、戦略上不可欠な取り組みへと進化してきました。それはなぜでしょうか。Moody's は2025年の調査でその理由として3つの重要な点を挙げています。

- 即時決済の普及により、不正行為とマネーロンダリングがほぼ同時に発生し得る状況になっていること。
- 不正行為が、AML調査に直接つながる前提犯罪として、重要性を増していること。
- 不正対策とコンプライアンスで別々のシステムを利用している金融機関では見通しが低下し、対応までに時間を要すること。

「AML関連事案の内訳で、発生件数が不正行為を上回るのは、麻薬取引のみです。」
SmartSearch 2024 マネーロンダリングおよび金融犯罪報告書

総合的にみると、これらの動向は明確な転換点を示しています。組織効率化の断続的な試みとして始まったものが、今や詐欺とAMLリスクが運用面、技術面、戦略面で深く絡み合っているという認識が業界全体に広がる段階に至りました。

環境変化

規制要因および政府の注力領域

Moody's によって特定された要因に加えて、規制当局は引き続き協調の必要性を重視しています。例えば、2025年に設立されたEUマネーロンダリング防止機関（AMLA）は、金融犯罪分野全体での監督の統合とインテリジェンスの共有を目的として設立され、加えて不正行為およびマネーロンダリングを含む複雑なスキームによって悪用される抜け穴を明示的に塞ぐことを目的としています。同様に、FinCENは2026年2月に内部告発者通報プログラムを開始し、既に把握されている、または疑いのあるマネーロンダリング違反や詐欺スキームの報告を奨励しています。

一方、シンガポールや英国などの管轄区域では、不正の補償に、特に注意を払って消費者保護規則が厳格化されています。シンガポールでは、共有責任フレームワークにより、特定の種類のフィッシング詐欺からの損失を詐欺被害者、金融機関、および携帯電話事業者の間で公平に分担することが義務付けられています。

また、英国の不正送金に関する返金制度の下では、銀行や電子決済会社を含むすべての決済サービスプロバイダーが、Faster Payments（訳者注：リアルタイム銀行振込ネットワーク）またはCHAPS（訳者注：高額かつ即時の銀行間資金決済システム）を通じて行われた承認されたプッシュ支払い（APP）詐欺の適格な被害者に補償を行わなければなりません。こうした「責任の転換」に加えて、本制度は、脆弱な立場にある顧客に対する追加的な保護措置も提供しています。消費者を標的とした不正行為が急速に増加していることから、消費者保護と補償に対する規制面での注目が一段と高まる可能性があります。

「金融不正の急速な拡大は、いわば「流行」とも言える状況にあり、その結果、個人（特に脆弱な立場にある人々）や法人が大規模かつグローバルな規模で被害に遭う事態を招いています。」
INTERPOL事務総長　Jürgen Stock

規制当局の取り組みにとどまらず、不正行為の蔓延は政府の最上位レベルでも注目を集めています。3月6日、トランプ大統領は「サイバー犯罪および不正行為との戦い」と題する大統領令に署名し、関係する政府機関に対し、不正行為やサイバー攻撃に対抗するためのツールを特定し、連携を強化するよう指示しました。この大統領令への署名は、金融サービス業界の幹部がこれらの犯罪への対応において、政府によるさらなる支援を訴えた下院金融サービス委員会の公聴会を受けて行われました。

英国においても、政府が3月に新たな不正対策戦略を発表するとともに、政府機関、情報機関、警察、銀行、携帯通信事業者、テクノロジー企業の専門家を結集する「オンライン犯罪センター」を立ち上げました。その目的は、データの共有やAIの活用を通じて連携を強化し、グローバルな不正ネットワークの全体像を把握することにあります。英国当局間の連携強化により、不正対策およびコンプライアンスの両面で、より深い協調体制が実現すると期待されています。

これらの政府の取り組みは、不正リスクの特定と対応において断片的なアプローチではもはや十分でないことを明確に示しており、このメッセージは金融機関にとっても重要なものと言えるでしょう。

不正の動向および犯行手口

金融機関の歴史を振り返れば、不正実行者は常に金融機関やその顧客を悪用しようとしてきました。現代の不正を巡る課題には、ソーシャルエンジニアリング、アカウント乗っ取り、マネー・ミュールネットワーク、リアルタイム決済を悪用した詐欺、ディープフェイクなどのさまざまな手法が含まれます。これらの手法は、既存システムの脆弱性を悪用するだけでなく、デジタルトランザクションへの依存度の増加やAIなどの技術の急速な進歩を背景に、より巧妙化しています。例えば、個人を誘導して機密情報を入手するソーシャルエンジニアリングは、近年、非常に一般的な手法となっています。

同様に、アカウント乗っ取りスキームは、正規の口座への不正アクセスを通じて、多くの場合、消費者と金融機関の双方に深刻な経済的損失をもたらします。これらの脅威ではいずれも、サイバー攻撃やデータ漏えいによって入手した情報を利用するケースが見られます。こうした不正行為の傾向が収斂していることは、コンプライアンス対応と不正防止を分断して捉えるアプローチが不十分であることを浮き彫りにしています。

金融機関とその顧客に影響を与える不正の種類

- APP（訳者注：金融送金詐欺）詐欺、ソーシャルエンジニアリング詐欺
- 小切手詐欺
- ローン詐欺
- フィッシング、スミッシング（訳者注：SNSフィッシング）、ビッシング（訳者注：音声フィッシング、ビジネスメール詐欺（BEC）を含む）
- アカウント乗っ取り詐欺
- ファーストパーティ詐欺（訳者注：本人の虚偽による不正）および合成ID詐欺
- P2P決済詐欺

不正行為がますます複雑化し、正当な取引と絡み合うようになるにつれて、金融機関はコンプライアンスと不正検知の両方を包含する包括的な視点を採用しなければなりません。

技術革新

デジタルID技術、人工知能および機械学習（AI/ML）、行動分析、最新のデータアーキテクチャにより、金融機関は歴史的に断片化されていたコンプライアンスと不正リスク管理の領域を統合することが可能になります。デバイスインテリジェンス、生体認証、本人確認プラットフォームなどを含むデジタルID管理・アクセス管理技術は、検知のための重要な追加機能を提供します。具体的には、顧客が実際に誰であるかを検証し、不正実行者やマネーロンダリングに関与する者によって悪用される、合成IDや改ざんされたIDがエコシステムに入り込む前に検知することで、重要なギャップを解消します。

AI/MLモデルは、構造化データおよび非構造化データを含む膨大なデータをリアルタイムで分析することにより、金融機関が疑わしい行動をより早期に、かつ高い精度で特定することを可能にします。これに行動分析を組み合わせることで、金融機関は単純なルールベースのアラートを超えて、顧客行動における微妙な異常を認識できるようになります。こうしたよりターゲットを絞ったアプローチは、AMLお

よび不正対応の双方における主要な非効率要因である誤検知を劇的に削減し、不正対策とコンプライアンスの双方に利益をもたらす共有の洞察を生み出します。

データレイクは、これらの機能を全体として有機的に連携させるための基盤として機能します。コンプライアンス、不正対策、オペレーション、クレジット、顧客チャネルに散在する孤立したデータセットの代わりに、データレイクは関連情報を一つの環境に統合し、一貫したガバナンスと柔軟なスキーマを提供します。この統一されたデータ基盤により、AIおよび分析ツールが顧客体験、取引フロー、リスク指標を同時に横断して分析できるようになります。これは、従来のアーキテクチャでは実現が難しかった点です。

その結果、金融機関は全社的なリスクスコアリング、共有アラートの生成・管理および部門横断型ダッシュボードを展開することができます。結果として、重複レビューを削減し、調査プロセスを加速する、より統合されたインテリジェンス主導のアプローチが得られます。最終的に、これらの技術は金融機関が受動的で孤立した統制から、能動的で協調的なリスク管理へと移行することを可能にし、コンプライアンスと不正対策の橋渡しを通じて、非効率を削減し、全体的なプログラムの有効性を向上させます。

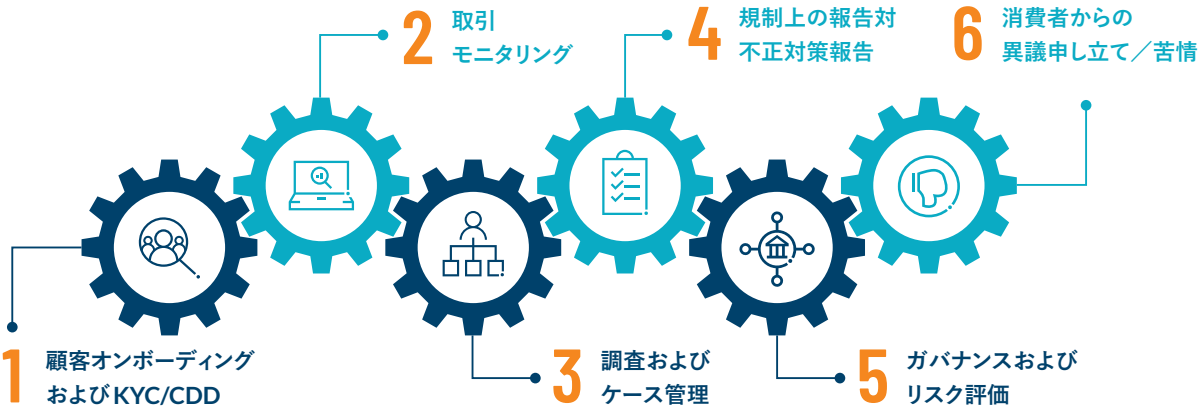
サイバーリスク

技術革新と密接に関連しているのは、サイバー攻撃の深刻化です。ボット攻撃などの組織化された自動化サイバー脅威を含む金融機関へのサイバー攻撃は、不正実行者に対し、不正取引を実行するために必要なアクセス権やデータを提供してしまいます。データ侵害やシステム侵入によって、顧客の機微情報が漏えいし、犯罪者がそれを利用してアカウントを乗っ取ったり、不正な送金を実行したりする事例が発生しています。近年では、AIを活用したサイバー攻撃がこの問題をさらに拡大させています。すなわち、不正実行者はディープフェイクやAIで高度化されたソーシャルエンジニアリング、精巧ななりすましを用いて行員や顧客を欺き、不正な支払いの承認や基本的なKYC（本人確認）統制の回避を図っています。

また、サードパーティのサービスプロバイダーに対するサイバー攻撃も、基幹プラットフォームの停止や統制の低下、さらには複数の金融機関への同時波及を通じて、不正が発生する構造的な隙を生み出します。これらの脆弱性が悪用されると、相互接続されたシステム間にて迅速に拡散する大規模な不正キャンペーンを可能にしてしまいます。

結論：不正行為を行う犯罪者は、AIの「民主化」や「武器化」によって悪意ある活動を高度化し続けており、不正とコンプライアンスを区別していません。規制当局もまた、両者を明確に切り分けて対応しているわけではありません。したがって、金融機関も区別すべきではないと言えるでしょう。今後、競争優位を確立する企業というのは、不正対策とコンプライアンスのリスク管理が共有する使命―すなわち、金融機関の健全性を守るという目的―を認識し、それを支える統合的なフレームワークを構築できる組織でしょう。

交差点となる領域：6つの重要な接点



6つの重要な接点

コンプライアンスと不正対策機能の融合は、金融機関のオペレーティングモデルにおける6つの重要な接点で最も顕著に現れます。これらの領域は、より強固で統合された防衛線を構築する上での課題であると同時に、重要な機会でもあります。

顧客オンボーディングは、金融犯罪コンプライアンス違反と不正行為の両方に対する第一の防衛線です。高度な文書認証と生体情報による確認を含む、徹底的かつ統合された本人性の保証・検証および文書認証は、KYC/CDD（本人確認・顧客管理）の要件を満たすだけでなく、合成ID詐欺の検知および防止にもつながります。同様に、共通のデータモデルをリスクスコアリングに活用することで、高リスク顧客を早期に特定でき、コンプライアンスと不正防止の双方の目的を支援します。不正検知ロジックをKYC／CDDの業務フローに組み込むことで、金融機関は、顧客受入時点での不正行為を抑制すると同時に、マネーロンダリングのリスクを低減することが可能となります。

取引モニタリングもまた、不正対策とコンプライアンスが重なる重要な領域であり、さらなる連携によって大きな効果が期待されます。両方の分野は、疑わしいまたは異常な取引パターンの分析において、類似するタイポロジーやアラートロジックを用いていますが、異なるモニタリングツールやプラットフォームを使用しているケースがよくあります。これにより、不正対策とAMLの双方の観点でアラートが発生し、同一の取引や行為に対して重複した対応が求められることがあります。しかし、データ共有や行動分析の活用により、コンプライアンス違反と不正スキームの双方を、より高い精度で検知することが可能になります。特に、リアルタイム決済や国際間取引が複雑化する中では、こうした連携はより有効に機能します。統合された取引モニタリングシステムは、迅速な手続とアラート疲労の軽減を通じて、より高度なリスク検知を可能にし、重要な脅威の見逃しを防止します。

疑わしい活動が検知されると、**調査とケース管理**がコンプライアンスおよび不正対策の両面における問題を解決するための焦点となります。従来、ケースは別々のプラットフォームで管理されることが多く、その結果、顧客へ重複して連絡し、調査結果が不整合となり、情報が欠損し、さらには照合作業における課題が生じてきました。統合型のケース管理プラットフォームは、調査の連携を可能にし、記録や証跡を一元管理するとともに、協調的なトリアージモデルを可能にします。こうしたプロセスの統合は、業務の相乗効果による運用コストの削減という付随的なメリットももたらします。このアプローチは、業務効率を高めるだけでなく、特定のシナリオのあらゆる側面を網羅した、一貫性と網羅性のある意思決定を可能にします。

報告義務は、AMLコンプライアンスと不正対応の境界が曖昧になるもう一つの領域です。例えば、疑わしい取引報告（STR）や疑わしい活動報告（SAR）、不正対策報告は、それぞれ異なるプロセスや基準で、国や金融機関によって異なるものの、通常は別々のチームによって対応されます。そのため、レビューされる情報は提起された問題に特化する傾向にあり、より広範な活動や過去の判断に対する精査は限定的になります。統合された報告フレームワークを導入することで、重複の削減、正確性の向上、人員配置や業務効率の改善が期待され、より包括的で示唆に富む報告につながります。

また、不正および**AMLに関するガバナンスやリスク評価**が重複することで、対応の実効性が低下する恐れもあります。統合されたガバナンス体制は、部門横断の連携を促進し、責任の明確化、課題に対するより深い理解、そして意思決定の一貫性を確保します。不正を含む金融犯罪リスクを単一のリスク分類体系として整理することで、金融機関はリスク環境をより的確に把握し、評価や対応の優先順位付けをより行いやすくなります。同様に、不正およびより広範な金融犯罪を対象として共同で全社的なリスク評価や顧客リスク評価を実施することで、新たに顕在化するリスクを特定し、測定し、関連するすべてのリスク要因にわたって適切に低減することが可能となります。

顧客からの異議申立てや苦情は、不正対策およびマネーロンダリング対策の双方に有益な潜在的なリスクや脆弱性を明らかにします。コンプライアンス担当と不正対策担当の双方が、苦情や異議申立てに関するデータを分析することで、システム上の課題や新たな不正トレンドを示す兆候を把握することができます。さらに、苦情対応を統合的に行うことで、迅速かつ一貫した解決が可能となり、顧客との摩擦を軽減できると同時に、根本原因の特定や統制強化にもつなげることができます。

歴史的な障壁

コンプライアンス機能と不正対策機能の融合が必要であるという認識は高まりつつあるものの、これまでの慣行や構造に起因する複数の障壁が、その進展を妨げてきました。中でも、文化的要因や規制上の課題は大きく、連携や業務効率性を制限するサイロ化を生み出してきました。

統合における主な障壁の一つは、不正対策とコンプライアンスの企業全体のチーム間に存在する文化的な隔たりです。不正対策チームは、損失の最小化や顧客満足の確保に重点を置く、第一線の業務機能として位置付けられることが多い一方、コンプライアンスチームは、法令・規制の遵守を担う第二線機能として設計されるのが一般的です。この違いにより、不正対策チームは迅速な業務対応を重視し、コンプライアンスチームはガバナンスやリスク管理を重視するという、両者の使命の対立を生み出します。場合によっては、こうした障壁が、統合に伴う権限や裁量の喪失への抵抗から生じるチーム間の争いを覆い隠す口実となることもあります。さらに、評価指標の不整合も、この分断を悪化させます。不正対策チームは損失削減や効率性で評価される一方、コンプライアンスチームは規制遵守の達成度で評価されるため、この摩擦が協調よりも孤立した運営を招く要因となります。

また、国や地域によって異なり、かつ継続的に変化する規制上の要請、とりわけ、第二線機能としての独立性を確保するという要請もまた、統合を難しくする要因となっています。コンプライアンス機能は、公正な監督を行うために第一線から独立して運営される必要がありますが、この点はガバナンス上不可欠である一方で、不正対策チームとの連携を難しくする側面もあります。これらの障壁はいずれも克服不可能なものではありませんが、フレームワーク、役割と責任、そして適切なガバナンスを慎重に設計する必要があります。

しかし、多くの金融機関にとって、統合に向けた障壁の中心には、基幹システムの刷新、AI／機械学習（AI/ML）活用を支えるためのクラウド移行、データのサイロ化やデータ欠損への対応、そして最高データ責任者、最高技術責任者、最高情報責任者といった追加的な社内関係者の関与などを含む、テクノロジーの近代化があります。テクノロジーは、不正対策とコンプライアンスの融合を可能にする中核的な要素であり、AI/MLや行動分析を活用した両機能に共通の分析基盤、統合されたデータアーキテクチャを金融機関に提供し、リアルタイム決済保護などの高度なツールを通じて脅威の検知から低減までに要する時間の短縮を実現します。

こうした課題への対応は、不正対策とコンプライアンスの統合にとどまらず、それをはるかに超える重要性を持っています。テクノロジーの近代化やデータのサイロ化・欠損への対処は、金融機関の将来における持続可能性の基盤そのものです。テクノロジー基盤やデータへのアクセスおよび活用能力を近代化できない金融機関は、コストの上昇、競争力の低下、そしてリスクの増大に直面することになります。

統合を妨げるレガシー的な考え方

- 不正対策とコンプライアンスは異なる使命を持ちます。不正対策の主な役割は財務的損失から組織と顧客を守ることにある一方、コンプライアンスの役割は法令・規制を遵守することです。
- コンプライアンスでは事後的な視点で活動を評価し、結論を裏付ける明確な監査証跡が求められます。一方、不正対策は悪意のある行為者を阻止し、財務的損失を防ぐために、リアルタイムまたはリアルタイムに近い対応が必要となり、コンプライアンスの文書化基準を満たすことは困難です。
- コンプライアンスは、結論を導くために顧客、取引相手、過去の活動に関する詳細な背景情報を必要とします。一方、不正対策はデバイスID、取引速度、位置情報、認証エラーなどの瞬間的な脅威に焦点を当てています。
- 不正対策は損失の阻止に重点を置き、コンプライアンスは報告と規制遵守を重視します。
- コンプライアンスには独立性の確保が求められるため、不正対策との統合が制約される場合があります。
- 不正対策とコンプライアンスは、それぞれ異なる当局への対応が求められており、各当局で求められるプロセスや期待値も異なります。
- 不正対策とコンプライアンスの調査担当者には、異なるスキルセットが求められます。
- 不正対策とコンプライアンスの調査を統合すると、対応スピードが低下するのではないかという懸念があります。

融合の利点

コンプライアンスと不正対策の機能を融合することで、金融機関は金融犯罪に対してより強力で一体的で全体的な防御を構築する機会を得ることができます。サイロ化を打破することで、組織は以下を含む重要な効果を得ることができます。

- **リスク検知能力の向上。**融合により、インテリジェンスの共有や、高度な分析を活用したリスクシグナル（レッドフラッグ）に関する洞察の高度化を通じて、金融機関は金融犯罪のライフサイクルのより早い段階で、かつより高い精度でリスクを検知できるようになります。さらに、統合された取引モニタリングと行動分析により、疑わしい活動の早期検知が促進され、金融機関が進化し続けるリスクに先んじて対応することが可能になります。こうした高度化された検知・分析能力は、AIの武器化と加害者の巧妙化によって増加している、合成ID不正やリアルタイム決済を悪用した不正などの高度な不正手法への対策において、特に重要です。

- **業務効率とコスト削減。**融合の最も即効性のある利点の一つは、プロセスやデータ管理、人的リソース最適化、調査プロセスの効率化における重複の削減です。これらの機能を統合することで、重複アラートや並行調査などの非効率が排除され、データや技術、人員を活用したより効率的な業務運営が可能となります。

- **顧客体験の向上。**オンボーディング時の重複や摩擦が減ることで、インテリジェンスや分析の共有が進み、誤検知が減少します。また、調査やケース管理を連携して行うことで、リスク評価の精度が高まるとともに、問題解決の迅速化も期待できます。

- **規制対応力（レジリエンス）の向上。**統合モデルは、組織の現在および将来的に変化する規制要件への対応力と柔軟性を高めます。その結果、一貫した正確な記録保持や明確な監督・説明責任を確保しつつ、規則やガイドラインへの準拠を明確に示すことが可能となります。

- **全社的リスクの低減。**より強靭で測定可能かつ持続可能な金融犯罪対策プログラムは、大規模な不正損失の発生可能性だけでなく、規制リスクや風評リスクの低減にも寄与します。

望ましい最終的な状態…そこに至るまでの道筋

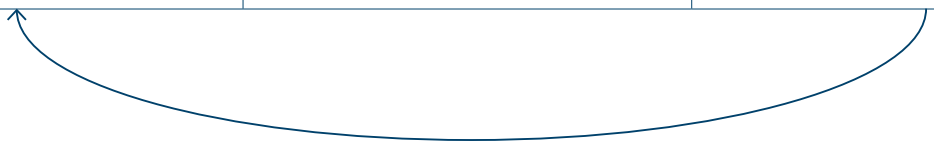
統合された金融犯罪およびコンプライアンスリスク管理フレームワーク（ここでは「全社的な脅威・金融犯罪・顧客インテグリティフレームワーク」と呼びます）の望ましい最終的な状態とは、サイバーリスク、金融犯罪（不正、AML、制裁を含む）、およびそれらに起因する消費者被害の管理において、共有されたガバナンス、標準化された手順、統合されたデータとテクノロジーのエコシステムによって、分断された形ではなく統合的なアプローチで管理することが可能な状態です。

この機能は最高金融犯罪責任者（Chief Financial Crimes Officer）が統括し、データサイエンティストやAI/ML領域の専門家、脅威インテリジェンスアナリスト、行動分析、詐欺対策の専門家、制裁対応の専門家、タイポロジー設計担当者、経験豊富な調査担当者、レッドチーム要員など、多様なバックグラウンドとスキルセットを持つ分野横断型のチームで構成されています。一部の組織では、スキルアップと新たな人材への投資の両方が必要となる場合もありますが、多くの金融機関では、これらの役割自体はすでに存在しているものの、サイロ化した状態で運用されているのが実態です。統合されたチームは、「認識」「対応」「報告」という三つの使命を持ち、あらゆる領域で疑わしい活動を認識・対応・報告します。

統合フレームワークの核心は、顧客および取引先の行動に対する全体的な視点を提供することであり、共通のデータレイク、高度なエンティティ解決、そして責任あるAIドリブン分析によって支えられています。これにより、疑わしい活動に対するリアルタイムの認識と対応が可能になります。統合フレームワークは内部および外部への報告も支援し、それらを通じた継続的な学習によって、組織のプログラムを強化するとともに、組織およびその顧客をより一層保護します。従来のサイロ型アプローチから統合フレームワークへの移行は、一部の組織にとって課題を伴うものとなります。

統合フレームワークの三つの使命

認識	対応	報告
• ホライズンスキャニング（新たに出現するタイポロジーや脅威インテリジェンスの把握） • 顧客管理および本人確認（ID不正を防止するための適切な対策を含む） • 統合されリスクスコアリングを組み込んだ取引モニタリングおよび融合されたケース管理により、レビュアーや調査担当者が、KYC・本人属性、取引モニタリング結果、不正インテリジェンス、位置情報の異常性、チャネル横断のパターンを一元的に把握可能になる	• リアルタイムでの介入（例えば、取引の謝絶、追加確認のための保留、顧客への通知、対抗措置の発動など）	• 統合された経営報告 • 疑わしい取引・活動の報告 • 法執行機関との連携



継続的な学習とフィードバックループ

一般的に、その移行プロセスは次の5つの段階を経て進みます。

1. **最小限の協力段階。**この段階にある組織は、SAR/STR提出などにて限定的な調整を行いますが、活動をさらに統合することの実益については十分に確信を持てていません。

2. **認識段階。**この段階にある組織は、不正、AML、制裁、サイバー、消費者保護リスクがますます共通のデータ、共通の関係者、共通の攻撃対象領域を共有しつつ、共通の検知アプローチや分析方法によって恩恵を受けていることを認識しています。ここでは、組織はしばしば部門横断的な作業グループを形成し、特定された疑わしい活動に関する情報を共有し、場合によっては、少なくともアドホックな共同調査を行います。

3. **調整段階。**この段階では、組織はプロセス、データ、分析の連携を開始しますが、組織構造の更新は行っていません。調整段階に進むためには、組織はアラートおよびケース管理プラットフォームを統合するか、少なくともリンクさせる必要があり、AI/MLを使用してその取り組みを支援する初期段階にある必要があります。

4. **統合段階。**この段階では、組織は最高金融犯罪責任者によって統括される統一フレームワークを正式に採用します。ここでは、インテリジェンスの共有、本人確認およびAMLチェック、取引モニタリング、ケース判断、報告がすべて完全に統合されています。

5. **最適化段階。**この最終段階では、組織は統一プラットフォームを使用して、顧客、取引相手、ID、デバイス、行動をシームレスに監視します。ここでの監視はリアルタイムで行われ、AI/MLモデルによる自律的な検知が可能となり、顧客オンボーディングがデジタルでサポートされ、顧客リスクスコアリングが動的に更新されます。さらに、顧客の苦情やサイバー事案が従来のAML、制裁、不正指標と統合され、リスクを包括的に把握できるようになります。

多くの金融機関にとって、融合に向けた取り組みは、既存の障壁への最適な対応方法を見極めながら、段階的に進めていく必要があります。金融機関全体においてコスト最適化が引き続き重要なテーマとなる中、業務効率の向上や財務損失の削減は、統合を推進する上で依然として有力な動機となります。

結論

最終的に、不正対策とコンプライアンス機能の統合に向けた移行は、単なる組織構造の見直しにとどまるものではありません。それは、分断ではなく協力を、サイロ化された情報ではなくインテリジェンスの共有を、そして組織上のチーム間の争いではなく消費者保護を選択するという、リーダーシップの意思決定に関わるものです。この考え方を受け入れる金融機関が、今後数年間における、信頼性が高く現代的な金融犯罪リスク管理がどのようなものであるかを定義するでしょう。

本稿の執筆には、プロティビティのマネージングディレクタであるConstantine BoyadjievおよびTom Giltrowが貢献しています。

著者について

Carol Beaumierは、プロティビティのリスク&コンプライアンス・プラクティスに所属するシニア・マネージング・ディレクタ。ワシントンD.C.を拠点に、30年以上にわたり、さまざまな業界の幅広い規制問題に携わってきました。プロティビティに入社する以前は、アーサーアンダーセンの規制リスクサービス部門のパートナーを務め、The Secura Groupのマネージングディレクタ兼創設パートナーとしてリスク管理サービス部門を率いていました。コンサルタント業務に就く以前は、米国通貨監督庁（Office of the Comptroller of the Currency：OCC）において、主に多国籍および国際的に活動する銀行の検査官として、そのほかにもOCC長官の上級秘書官、OCC経営チームメンバーやOCC長官の庁内外渉外責任者として、11年間勤務しました。ボーミエは、規制やその他のリスク問題に関して頻繁に執筆や講演を行っています。

Bernadine Reeseは、プロティビティのリスク・コンプライアンス部門のマネージングディレクタ。ロンドンを拠点とするリースは、KPMGの規制サービス部門から2007年にプロティビティに入社。30年以上にわたり、さまざまな金融機関のクライアントと共に、リスク、コンプライアンス、ガバナンスの変革を成功裏に実行し、これらの業務を最適化することでビジネスパフォーマンスを向上させてきました。認定気候リスク専門家（Certified Climate Risk Professional）でもあります。

プロティビティのコンプライアンスリスクサービスについて

規制遵守の負担を管理する、より良い方法があります。各機能が事業目標と整合し、プロセスが最適化され、手続がデータとテクノロジーによって自動化・簡易化されたとしたらどうでしょうか。規制要件は、より効率的に満たされ、統制は事後対応型ではなく予測型へと進化します。従業員は自身の役割からより高い価値を得られるようになり、企業はレピュテーションが守られているという安心感のもと、成長とイノベーションにより注力することが可能になります。

プロティビティは、コンプライアンスをアジャイルリスクマネジメント・チームに統合し、フォワードルッキングかつ予測型の統制を実現するために分析を活用するとともに、規制コンプライアンスに関する専門知見を適用しています。また、規制当局による是正措置やコンプライアンス上の課題への対応をより効率的に進めるための自動化されたワークフローツールの活用、新商品・新サービスにおける顧客ニーズおよびコンプライアンス要件の設計要件への落とし込み、さらに規制コンプライアンスの実施状況を継続的にモニタリングするための仕組みの構築を通じて、組織を支援しています。

protiviti®